

ATTORNEY DOCKET NO.
073897.0158

PATENT APPLICATION
10/759,960

1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED

MAY 27 2005

Technology Center 2100

In re Application of: Richard A. Braun et al.
Serial No. 10/759,960
Filed: January 16, 2004
Title: System and Method for a Directory Secured User Account

MAIL STOP: TECHNOLOGY CENTER 2100
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

<p style="text-align: center;">EXPRESS MAIL</p> <p>Express Mailing Label Number EV 733638951 US</p> <p>I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.</p> <p><i>Willie Jiles</i> _____ Willie Jiles</p> <p>Date: May 24, 2005</p>

Renewed Petition Under 37 C.F.R. § 1.102(d)

In response to the Dismissal of Applicants' original Petition, Applicants submit this Renewed Petition to Make this Application special under 37 C.F.R. § 102(d). The Dismissal is attached hereto as Exhibit A.

Regarding Requirement B noted in the Dismissal, Applicants state that Applicants will make an election without traverse as a prerequisite to the grant of special status if the Office determines that all the claims are not obviously directed to a single invention. Regarding Requirement E noted in the Dismissal, Applicants provide below a revised discussion of the references. Applicants also discuss below additional references not in Applicants' original Petition.

Pre-Examination Search

The professional search firm Intellectual Property Concerns, Inc., made a pre-examination search. The search included Class 707, Subclass 3; Class 709, Subclasses 225, 226, and 228; Class 712, Subclasses 30 and 31; and Class 713, Subclasses 200, 201, and 202. The search firm also searched foreign patents and literature. The search firm consulted U.S.P.T.O. Examiner Peeso from Art Unit 2132 during at least certain portions of the search.

The search uncovered the following references:

1. U.S. Patent No. 6,009,455
Inventor: John F. Doyle
Title: *Distributed Computation Utilizing Idle Networked Computers*
2. U.S. Patent No. 6,418,462
Inventors: Yongyong Xu
Title: *Global Sideband Service Distributed Computing Method*
3. U.S. Patent No. 6,112,225
Inventors: Reiner Kraft, Qi Lu, and Marat Wisebond
Title: *Task Distribution Processing System and the Method for Subscribing Computers to Perform Computing Tasks During Idle Time*
4. U.S. Patent Application Publication No. US2002/0007394
Inventors: Phillip Andre Bertolus and Timothy Grant Lewis
Title: *Retrieving and Processing Stored Information Using a Distributed Network of Remote Computers*
5. U.S. Patent Application Publication No. US 2002/0091751
Inventors: Bradley M. Firlie
Title: *Distributing Computing*
6. U.S. Reissued Patent No. US RE37,811
Inventors: Gerard Sitbon, Francois Urbain and Therese Saliba
Title: *Distributed Application Load Distribution Aid Tool*
7. U.S. Patent No. 5,881,225
Inventor: Erik K. Worth
Title: *Security Monitor for Controlling Functional Access to a Computer System*

8. U.S. Patent No. 6,055,637
Inventors: Jerome D. Hudson et al.
Title: *System and Method of Accessing Enterprise-Wide Resources by Presenting to the Resource a Temporary Credential*
9. U.S. Patent No. 6,088,679
Inventors: John Barkley
Title: *Workflow Management Employing Role-Based Access Control*
10. U.S. Patent No. 6,141,778
Inventors: Kevin J. Kane et al.
Title: *Method and Apparatus for Automating Security Functions in a Computer System*
11. U.S. Patent No. 6,453,353
Inventors: Teresa Win et al.
Title: *Role-Based Navigation of Information Resources*
12. U.S. Patent No. 6,601,175
Inventors: Todd Weston Arnold et al.
Title: *Method and System for Providing Limited-Life Machine-Specific Passwords for Data Processing Systems*
13. U.S. Patent Publication No. US 2002/0046352
Inventor: George Stone Ludwig
Title: *Method of Authorizing by Proxy within a Computer Network*
14. U.S. Patent Publication No. US 2003/0018910
Inventors: Brian W. Wert et al.
Title: *System and Methods for Providing Multi-Level Security in a Network at the Application Level*
15. U.S. Patent Publication No. US 2002/0165758
Inventors: John R. Hind et al.
Title: *Identification and Tracking of Persons Using RFID-Tagged Items*
16. U.S. Patent Publication No. US 2003/0163566
Inventors: Gregory E. Perkins et al.
Title: *Data Access in a Distributed Environment*

Detailed Discussion of the References

U.S. Patent No. 6,009,445 discloses a system and method to utilize the otherwise unproductive minutes and hours when a networked client computer is not in use by a local human operator. The method and system allow multiple partitioned computations to be queued for distribution to any number of client computers when the clients indicate their availability. Availability may be determined by the same criteria used to activate screen-saver programs, i.e., a predetermined time without any keyboard or mouse input. Application programs are designed to accept a common calling sequence. An application-independent master control program coordinates the distribution of computation segments, the combination of partial results, and the formatting of the final result. An application-independent client control program reports availability of client computers, downloads application program files, invokes the application to compute partial results for a range of computation segments, and uploads the partial results to the master computer. One class of distributed computation supported is finding the minimum or maximum value of a calculated target cell in a spreadsheet, based on a number of input cells taking values within a specified range. Distributed computations can include searches of databases or searches of intranets or the Internet.

U.S. Patent No. 6,418,462 discloses a method of distributing computing, sideband computing, that is global, scalable and can utilize many idle CPU resources worldwide. Sideband is defined as when a user connects to some (normal) network services, a separate communication channel is opened, through which a server distributes its tasks to all the clients and collects the results later. By this method, any network server which has a lot of clients can compute very large parallel computing problems by dividing it into small individual parts and have them calculated by its clients. With little cost, the network server can act as a supercomputer. The sideband computing method can be extended to other distributed services such as distributed testing or distributed searching. Any computer, with the willingness to accept those tasks from outside, to be exposed to the public and to work for

anyone on the Internet, can earn credits (at idle times, normally). And network servers can contact those clients if they need more computing power.

U.S. Patent No. 6,112,225 discloses that a computer executable “aggregate” task is processed by dividing it into subtasks and distributing the subtasks “on demand” to remotely located subscribing computers via a computer network. The aggregate task originates at a coordinating computer, coupled to one or more peripheral computers by appropriate communications links. The coordinating computer divides the aggregate task into multiple independent subtasks. Each peripheral computer begins to “subscribe” to the coordinating computer’s aggregate task by obtaining an “idle time activation program” from the coordinating computer, and then installing the program locally. The idle time activation program which may include a screen saver, activates automatically when the subscribing computer is inactive. Continuing the subscription process, each peripheral computer requests a subtask from the coordinating computer. In response, the coordinating computer distributes different subtasks among the subscribing computers, completing the subscription process. The subscribing computers automatically work on their respective subtasks whenever they are idle, as directed by the local idle time activation program. When a subscribing computer completes its subtask, it transmits results back to the coordinating computer. When results of all subtasks have been received from subscribing computers, the coordinating computer compiles and stores these results, concluding the aggregate task.

U.S. Patent Application Publication No. US 2002/0007394 discloses a system that retrieves and processes information stored on computers connected by a communications network. A central computer receives notification from a remote computer that the computer is available to receive data. In response to that notification, the central computer sends address data to the remote computer. To utilize the available network resources with maximum efficiency, the central computer optimizes performance of the distributed system by allocating address data to the remote computer based on at least one characteristic of the remote computer, such as a measure of network connectivity and/or a performance

characteristic of the remote computer. This allocation may take place in accordance with the relative importance of the data for indexing purposes. The remote computer uses a communication interface connected to the Internet to retrieve the information stored at the locations specified by the address data, and stores that information. The remote computer then processes the retrieved information to generate processed data, and stores the processed data. Finally, the remote computer sends the processed data to the central computer. Just as the quality of information stored at different locations differs widely, so too do the characteristics and attributes of the remote computers which participate in most distributed computing systems. In particular, the quality (in terms of speed and power) and the network connectivity of the remote computers (relative to the information to be accessed and indexed) differ widely. Each computer has a certain amount in common, for example they generally all have a microprocessor, some form of memory, some form of input/output device, a network interface, and a storage device. Important areas in which they differ, however, include processor speed, storage capacity, reliability, average amount of idle time, time spent connected to a network, their proximity in the network to information that is to be indexed, and the speed of their network connection. Each of these points of difference can affect the contribution a computer can make to a distributed computing system. Accordingly, the present invention optimizes search engine performance by utilizing the unused processing capacity of networked remote computers to retrieve and process stored information on the Internet, and by doing so in a way which seeks to match the tasks to be processed with the most suitable computers available at the time, without incurring undesirably high communication costs.

U.S. Patent Application Publication No. US 2002/0091752 discloses distributed processing methods and systems that can coordinate and administer the execution of large-scale processor intensive computer models and data analysis used in problem solving. A server initiates a task to an administration module that can decompose the task into parts, or subtasks. The server can assign the subtasks to remote computers, or helpers, and collect the results of those subtasks from the helpers. The helpers can obtain the necessary processing

code from the administration module in the form of dynamically linked libraries (DLLs). Data to be processed can be obtained from local or remote data sources. Distributed computing is gaining popularity as a technique for harnessing idle computing power available through large networks such as the Internet. One such example is the Search for Extraterrestrial Intelligence ("SETI"), a project in which millions of computers connected to the Internet process astronomical data in an effort to identify signs of extraterrestrial life. However, existing approaches are typically limited to a specific problem for which client-side software may be downloaded to a number of participating computers, or to a particular type of problem for which processing tasks for clients are known in advance, so that participating computers may be pre-programmed to respond to specific processing requests.

U.S. Reissued Patent No. US RE37,811 discloses an invention relating to a toolkit for balancing the load of an application distributed among several machines belonging to a distributed data processing system in a local area network. A tool at the service of a distributed application running on machines of a distributed data processing system running in a local area network, intended for balancing the load on each of the machines of the system, includes a master daemon and a plurality of agent demons. The master and each of the agents calculate the load of the machines on which they are running. The master collects the load data of each of the agents at a first sampling interval and sends that collected load data to all of the agents. At the request of the distributed application, the local agent closest to the application indicates to the application which machine has the lightest load. The application then makes the decision to request the machine with the lightest load to execute the services the application requires. As necessary, the tool selects a master from the agents, thereby ensuring the existence and uniqueness of a master at all times, regardless of failure affecting one or more machines in the data processing system.

U.S. Patent No. 5,881,225 discloses security functions for a computer system controlled by a security monitor. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from

among one or more roles defined in the system. Upon being validated as an authorized user performing a particular role, the user is then authorized to perform certain functions and tasks specifically and to see information associated with that role (and optimally the work group the user is assigned). For some users, no role or a “null” roll is chosen, and authorization for certain functions and tasks is accomplished due to that particular user having been predefined by an administrator as being allowed to perform those functions and tasks, usually due to the predefined privileges associated with the work group(s) to which the user belongs.

U.S. Patent No. 6,055,637 discloses a resource access control system and method for a corporate enterprise that includes a security administrator in communication with multiple users. Each of the users have an assigned role and a unique user identifier. A temporary credential token is generated correlative to the assigned role of the user by the security administrator as the user logs on by entering the assigned unique user identifier and indicates a desire to access a resource. The temporary credential token is communicated to the resource and any subsequent resources to allow access by the user and deleted as the user terminates the session.

U.S. Patent No. 6,088,679 discloses a workflow sequence specified by a process definition managed by a workflow management system which enacts each segment in the order specified by that process definition. Role-based access control (RBAC) is used to define membership of individuals in groups, i.e., to assign individuals to roles, and to then activate the roles with respect to the process at appropriate points in the sequence. Any individual belonging to the active role can perform the next step in the business process. Changes in the duties and responsibilities of individuals as they change job assignments are greatly simplified, as their role memberships are simply reassigned; the workflow process is unaffected.

U.S. Patent No. 6,141,778 discloses a computer security system automatically that updates an access status and a level of access privilege for each user based on outside feeds

related to current status of the user with respect to an organization, such as a business or school and the membership of the user in a group or department within the organization. A unique user identifier is assigned to each user across all computing systems. The computing system retains the relationship between the user and the user identifier even after the user's access to the computing system is terminated. The user may be reassigned the same user identifier should the user again be granted access to the system resources. The computing security system may be implemented as an overlay to an existing resource allocation system, such as the RACF system commonly found on many mainframe computers and may allow decentralization of certain security functions.

U.S. Patent No. 6,453,353 discloses a single secure sign-on that gives a user access to authorized Web resources, based on the user's role in the organization that controls the Web resources. The information resources are stored on a protected Web server. A user of a client or browser logs in to the system. A runtime module on the protected server receives the login request and intercepts all other request by the client to use a resource. The runtime module connects to an access server that can determine whether a particular user is authentic and which resources the user is authorized to access. User information is associated with roles and functional groups of an organization to which the user belongs; the roles are associated with access privileges. The access server connects to a registry server that stores information about users, roles, functional groups, resources, and associations among them. The access server and registry server exchange encrypted information that authorized the user to use the resource. The user is presented with a customized Web page showing only those resources that the user may access. Thereafter, the access server can resolve requests to use other resources without contacting the registry server. The registry server controls a flexible, extensible, additive data model stored in a database that describes the user, the resources, roles of the user, and functional groups in the enterprise that are associated with the user.

U.S. Patent No. 6,601,175 discloses features of a data processing system, such as its configuration, protected utilizing a machine-specific limited-life password. The data

processing system includes execution resources for executing a watchdog program, a limited-life value generator, and non-volatile storage that stores a machine-specific value at least partially derived from relatively unique information associated with the data processing system (and preferably also derived from a secret control password). In response to each attempted access to the protected features of the data processing system, the watchdog program generates at least one machine-specific limited-life password from the machine-specific value and a limited-life value generated by the limited-life value generator. The watchdog program allows access to the protected features in response to entry of the machine-specific limited-life password and otherwise denies access. Depending upon implementation, the limited-life value can represent a timestamp that limits the duration that the machine-specific limited-life value is valid or a nonce that limits the number of times that the machine-specific limited-life value can be used.

U.S. Patent Publication No. 2002/0046352 discloses a method for enabling participants in an information technology (IT) system or a computer network to delegate user authority to other system participants. The method includes the generation of a proxy authorization. The proxy authorization, or proxy, is used by the IT system to insure that a given participant may have access to resources on the basis of a permission granted and intended by another user or agent of the IT system and that the grantor of the permission is authorized to issue the access and authorities as designated by or within the proxy authorization. A medical record repository, for example, may allow unlimited access to particular individual patient records to an individual medical doctor. The doctor can then authorize a specific pharmacy to have limited access to designated portions of the medical records of certain of the patients to whom the doctor is authorized access. The pharmacy may then allow access to distinct and different subsets of the portions of the records, to which the pharmacy is authorized access to by a proxy issued by the doctor, to an insurance company, to a billing clerk, and to pharmacists. The use of proxies thereby allows for efficient B2B collaborative message processing using languages such as XML.

U.S. Patent Publication No. 2003/0018910 discloses systems and methods for providing multi-level security for a software application. In one system, an application programming interface provides access to secured software applications. A database stores authorizations granting each user access to selected applications, selected application screens, and selected fields within application screens. The application programming interface is configured such that a security software application prevents a user from gaining access to an application, screen, or field unless authorization has previously been given. A further system provides for the assignment of privileges to users of the application. These privileges define the specific functions that a user is allowed to perform with respect to an authorized application, screen, or field.

U.S. Patent Publication No. 2003/0163566 discloses a method and system for providing a first network resource limited access to a second network resource. The method includes receiving profile data. Using the profile data, temporary credentials are then generated for accessing the second network resource. The temporary credentials are then made available to the first network resource. The temporary credentials are invalidated following a termination event such as the lapse of a set time period or after the second resource has been accessed.

Applicants' Claims are Patentable Over the Above References

The above references, whether considered individually or in any combination, fail to disclose, teach, or suggest one or more limitations recited in Applicants' claims. As an example, the references fail to disclose, teach, or suggest "providing an access token to the available network resource, the access token operable to allow an application of the available network resource to access a portion of the network" and "tracking the status of the access token," as recited in independent Claim 1. As another example, the references fail to disclose, teach, or suggest "an administrator, the administrator operable to identify at least one available network resource, provide the access token to the at least one available network

resource, and store a status corresponding to the access token,” as recited in independent Claim 26. As another example, the references fail to disclose, teach, or suggest “a resource communication module operable to transmit the at least one access token to a resource coupled to the network” and “a token management module operable to maintain the status of the at least one access token and the resource,” as recited in independent Claim 42.


Conclusion

Under 37 C.F.R. § 1.102(d), Applicants respectfully requests that this Application be granted special status. Should this Renewed Petition require any further support, please contact Jay B. Johnson, Attorney for Applicants, at 214.953.6431.

Applicants believe no fee is due. Nonetheless, the Commissioner is hereby authorized to charge any fee and credit any overpayment to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants



Jay B. Johnson
Reg. No. 38,193

Date: May 24, 2005

Correspondence Address:

Customer Number 05073